

IN THE CLAIMS

Please CANCEL claims 2 and 11, without prejudice or disclaimer. Please amend claim 3, as follows. A status of the claims follows.

Claim 1: (Original) A method of securely delivering data, comprising the steps of:

creating a container having electronic content and a container identifier;

encrypting at least one data block of the electronic content using a symmetric encryption technique and encrypting a header associated with a first data block of the electronic content using an asymmetric encryption technique, the header including a symmetric decryption key; and

re-keying the header using data associated with a user or a user's device to lock at least a portion of the electronic content to the user or the user's device,

wherein the locked at least a portion of the electronic content can only be decrypted and accessed by the user or on the user's device when the user or user's device has been authenticated against at least the container identifier.

Claim 2: (Cancelled)

Claim 3: (Currently amended) A computer program product comprising a computer usable medium having readable program code embodied in the medium, the computer program product includes at least one component to:

create a container having electronic content and a container identifier;

determining determine at least one data block for partitioning the electronic content;

encrypt the at least one data block of the electronic content using a symmetric encryption technique and to encrypt a header associated with a first data block of the electronic content using an asymmetric encryption technique, the header including a symmetric decryption key;

re-key the header using data associated with a user or a user's device to lock at least a portion of the electronic content to the user or the user's device, wherein the locked at least a portion of the electronic content can only be decrypted and accessed by the user or on the user's device when the user or user's device has been authenticated against at least the container identifier; and

decrypt the locked portion of the electronic content when the user or user's device has been authenticated.

Claim 4: (Previously presented) The method of claim 1, further comprising the steps of:

requesting authorization to access the electronic content; and
receiving authorization to access the electronic content.

Claim 5: (Previously presented) The method of claim 4, further comprising re-keying the header based on each occurrence of the requesting step.

Claim 6: (Previously presented) The method of claim 5, wherein the re-keying the header step results in a different value for each occurrence of the re-keying step.

Claim 7: (Previously presented) The method of claim 1, wherein the electronic content includes at least any one of text, executable code, video, photos, and sales solicitations.

Claim 8: (Previously presented) The method of claim 1, wherein the step for re-keying occurs at the user's device.

Claim 9: (Previously presented) A computer-implemented method of securely delivering data, comprising the steps of:

creating a container having electronic content and a container identifier;

encrypting at least one data block of the electronic content using a symmetric encryption technique and encrypting a header associated with a first data block of the electronic content using an asymmetric encryption technique, the header including a symmetric decryption key; and

re-keying the header using at least a portion of the container identifier and data associated with a user or a user's device to lock at least a portion of the electronic content to the user or the user's device,

wherein the locked at least a portion of the electronic content can only be decrypted and accessed by the user or on the user's device when the user or user's device has been authenticated against at least the container identifier, and

wherein the step for re-keying creates a unique value for the header for every different container delivered to the user's device.

Claim 10: (Previously presented) The computer-implemented method of claim 9, wherein the step for re-keying occurs at the user's device.

Claim 11: (Cancelled)

Claim 12: (Previously presented) A computer-based method for accessing content, the method comprising the steps of:

transmitting an electronic container having files of electronic content and a container identifier, wherein at least one data block of the electronic content is encrypted using a symmetric encryption technique and a header associated with a first data block of the electronic content is encrypted using an asymmetric encryption technique, the header including a symmetric decryption key; and

transmitting a permission token based on an attempt to access the electronic content to grant access to the electronic content, wherein at least the symmetric decryption key is re-encrypted for each occurrence of transmitting the permission.

Claim 13: (Previously presented) The computer-based method of claim 12, wherein the container identifier and device indicia is used to re-encrypt at least the symmetric decryption key for each occurrence of transmitting the permission for locking the electronic content to a device having the device indicia.

Claim 14: (Previously presented) The computer-based method of claim 12, wherein a container identifier and device indicia is used to re-encrypt the header.

Claim 15: (Previously presented) The computer-based method of claim 12, wherein the electronic container includes at least any one of: executable code, text, video, photos, audio, financial data, and sales solicitations.

Claim 16: (Previously presented) The computer-based method of claim 12, wherein the attempt to access the electronic content occurs at a user's computing device.